(51) International Patent Classification:
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/CN2005/002386

(22) International Filing Date:
30 December 2005 (30.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95054 (US).

(72) Inventor; and
(75) Inventor/Applicant (for US only): ZHANG, Peng [CN/CN]; Room 402, No.122, Hangxin Road, Shanghai 201105 (CN).

(74) Agent: INTELLECPRO CHINA LIMITED; 11/F, Tower C, Five Buildings, 9 Chegongzhuang Dajie, Xicheng District, Beijing 100044 (CN).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
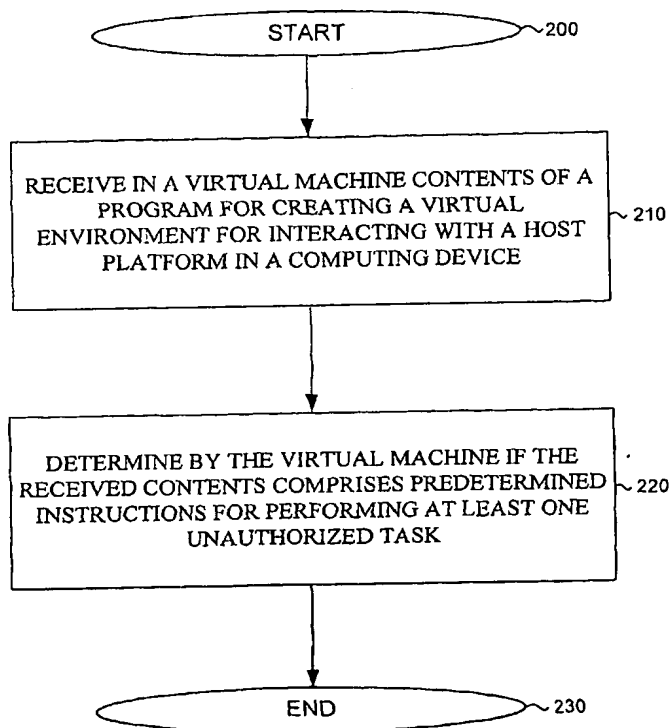
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

[Continued on next page]

(54) Title: VIRTUAL MACHINE TO DETECT MALICIOUS CODE

(57) Abstract: One embodiment of the invention discloses a method for receiving in a virtual machine(VM) contents of a program for creating a virtual environment for interacting with a host platform in a computing device; and determining by the VM if the received contents comprise predetermined instructions for performing at least one unauthorized task. Another embodiment of the invention discloses a method for receiving a system call for a host platform in communication with a VM of a computing device; and determining by the VM if the received system call comprises at least one predetermined system call for performing at least one unauthorized task. Yet another embodiment of the invention discloses a method for receiving a virtualized memory address for a host platform in communication with a VM of a computing device; and determining by the VM if the received virtualized memory address comprises at least one predetermined unauthorized virtualized memory address.

START ~200

RECEIVE IN A VIRTUAL MACHINE CONTENTS OF A PROGRAM FOR CREATING A VIRTUAL ENVIRONMENT FOR INTERACTING WITH A HOST PLATFORM IN A COMPUTING DEVICE ~210

DETERMINE BY THE VIRTUAL MACHINE IF THE RECEIVED CONTENTS COMPRISES PREDETERMINED INSTRUCTIONS FOR PERFORMING AT LEAST ONE UNAUTHORIZED TASK ~220

END ~230

WO 2007/076624 A1

WO 2007/076624 A1